The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

9/10/2013

SUBJECT:

Multiple Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (MS13-073)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Office Excel, a spreadsheet application provided my Microsoft. These vulnerabilities could allow remote code execution if a user opens a specially crafted Excel file. The file may be received as an email attachment, or downloaded via the web. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Microsoft Excel 2003
- Microsoft Excel 2007
- Microsoft Excel 2010
- Microsoft Excel 2013
- Microsoft Office 2011 for Mac
- Microsoft Excel Viewer
- Microsoft Office Compatibility Pack

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:

Three vulnerabilities have been discovered in Microsoft Excel.

Two Memory Corruption Vulnerabilities (CVE-2013-1315, CVE-2013-3158) are caused by the way that Microsoft Excel parses content in Excel files. Attackers could exploit these two vulnerabilities to gain the same rights as the current user. Attackers that successfully exploit this vulnerability could take complete control over the affected system. The attackers could then install programs; view, change, or delete data; or create new accounts with full user rights.

A third vulnerability (XML External Entities Resolution CVE-2013-3159) is caused by the way that Microsoft Excel parses specially crafted XML files containing external entities. Successful exploitation of this vulnerability could allow attackers to read data from files located on the targeted system. The above vulnerabilities can be exploited by opening malicious Excel files received as email attachments, or by visiting websites that host malicious Excel documents.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Microsoft:

http://technet.microsoft.com/en-us/security/bulletin/ms13-073

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1315

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3158

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3159

SecurityFocus:

http://www.securityfocus.com/bid/62167

http://www.securityfocus.com/bid/62219